On the Structure of Additive Quantum Codes and the Existence of Nonadditive Codes

Vwani P. Roychowdhury* Farrokh Vatan†
Electrical Engineering Department
UCLA
Los Angeles, CA 90095

Abstract

We first present a useful characterization of additive (stabilizer) quantum error–correcting codes. Then we present several examples of nonadditive codes. We show that there exist infinitely many non-trivial nonadditive codes with different minimum distances, and high rates. In fact, we show that nonadditive codes that correct t errors can reach the asymptotic rate $R = 1 - 2H_2(2t/n)$, where $H_2(x)$ is the binary entropy function. Finally, we introduce the notion of *strongly* nonadditive codes (i.e., quantum codes with the following property: the trivial code consisting of the entire Hilbert space is the only additive code that is equivalent to any code containing the given code), and provide a construction for an ((11,2, 3)) strongly nonadditive code.

1 Introduction

Almost all quantum error–correcting codes known so far are additive (or stabilizer) codes. An additive code can be described as follows. Consider the group $\mathcal{G}$ of unitary operators on the Hilbert space $\mathbb{C}^{2^n}$ defined by the tensor products $\pm M_1 \otimes M_2 \otimes \cdots \otimes M_n$, where each

*e–mail: `vwani@ee.ucla.edu`

†e–mail: `vatan@ee.ucla.edu`

M_i is either the identity $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or one the Pauli matrices σ_x, σ_z, or $\sigma_y = \sigma_x \sigma_z$. Then an additive code is a subspace $\mathcal{Q}$ of $\mathbb{C}^{2^n}$ for which there is an Abelian subgroup H of $\mathcal{G}$ such that every vector of $\mathcal{Q}$ is a fixed point of every operator in H [3, 4, 7]. This approach leads to a close connection between self–orthogonal (under a specific inner product) linear binary codes and additive codes, such that the minimum distance of the additive code is determined from the binary code.

It is natural to ask whether there is any quantum error–correcting code that can not be constructed in this way, directly or via some equivalence. We should make here a comment on the correct formulation of this question. Since the dimension of every additive quantum code is a power of 2, any quantum code whose dimension is not a power of 2 is not additive or equivalent to an additive code; specially, any subspace of an additive code with dimension not a power of 2 is a nonadditive code. We call such codes *trivial nonadditive codes.* But we prove a general theorem which shows that infinite families of non-trivial nonadditive codes with different values of d exist. The nonadditiveness of these codes does not follows from their dimensions (the dimensions of these codes are also powers of two), but from their very special structure. Moreover, we show that these nonadditive codes asymptotically reach the same rate as Calderbank–Shor–Steane codes.

We also propose the notion of *strongly nonadditive* codes: a quantum code $\mathcal{Q}$ is strongly nonadditive if the trivial code $\mathbb{C}^{2^n}$ is the only additive code that contains any code equivalent to $\mathcal{Q}$. Now the interesting problem is to find strongly nonadditive quantum codes. Recently in [13] it is shown that a $((5, 6, 2))$ strongly nonadditive code exists, which is better than any $((5, K, 2))$ additive code. Later in [12], Rains showed that there exists $((2m, 4^{m-1}, 2))$ nonadditive code, for all $m \geq 3$. We present an $((11, 2, 3))$ strongly nonadditive code.

In Section 3 we give a characterization of additive codes. This characterization is based on the special structure of some basis of the code, and provides an intuition for constructing the non-additive codes of Section 4.2. Finally, in Section 4 first we find a criterion that guarantees additiveness and strongly nonadditiveness of quantum codes then we present our example strongly nonadditive code. Moreover, we give more examples of nonadditive codes; we conjecture these codes are also strongly nonadditive.

2 Preliminaries

Consider the Hilbert space $\mathbb{C}^{2^n}$ with its standard basis $|v_1\rangle, \ldots, |v_{2^n}\rangle$, where $v_1, \ldots, v_{2^n}$ is a list of binary vectors of length n in $\{0,1\}^n$. For every binary vector α of length n, we define the unitary operators X_α and Z_α by following equations

$$\begin{aligned} X_\alpha |v_i\rangle &= |v_i + \alpha\rangle , \\ Z_\alpha |v_i\rangle &= (-1)^{v_i \cdot \alpha} |v_i\rangle . \end{aligned}$$

Note that $X_\alpha Z_\beta = (-1)^{\alpha\cdot\beta} Z_\beta X_\alpha$.

Let $\mathcal{G}$ be the group of all unitary operators of the form $\pm M_1 \otimes \cdots \otimes M_n$, where $M_i \in \{ I, \sigma_x, \sigma_y, \sigma_z \}$. Then every member of $\mathcal{G}$ can be represented uniquely as $(-1)^\lambda X_\alpha Z_\beta$, where $\lambda \in \{0,1\}$ and $\alpha, \beta \in \{0,1\}^n$. For every subset $\mathcal{S}$ of $\mathcal{G}$, let $\overline{\mathcal{S}} \subset \{0,1\}^{2n}$ be the set of all vectors $(\alpha|\beta)$ such that either $X_\alpha Z_\beta \in \mathcal{S}$ or $-X_\alpha Z_\beta \in \mathcal{S}$. We say $\overline{\mathcal{S}}$ is *totally singular* if for every $(\alpha|\beta) \in \overline{\mathcal{S}}$ we have $\alpha \cdot \beta = 0$. We also define a special inner product on $\{0,1\}^{2n}$ as

$$((a|b), (a'|b')) = a \cdot b' + a' \cdot b, \tag{1}$$

where the right–hand side is evaluated in GF(2). For any quantum code $\mathcal{Q}$ in $\mathbb{C}^{2^n}$, we define the *stabilizer* $\mathcal{H}_\mathcal{Q}$ of $\mathcal{Q}$ as

$$\mathcal{H}_\mathcal{Q} = \{ \varphi \in \mathcal{G} : \varphi |x\rangle = |x\rangle \text{ for every } |x\rangle \text{ in } \mathcal{Q} \} .$$

Then it is easy to check that $\mathcal{H}_\mathcal{Q}$ is an Abelian group and every element of $\mathcal{H}_\mathcal{Q}$ squares to the identity operator. So $\overline{\mathcal{H}_\mathcal{Q}}$ is totally singular. It also follows that $\mathcal{H}_\mathcal{Q}$ is isomorphic to a vector space $\mathrm{GF}(2)^m$, for some m. This means that $\mathcal{H}_\mathcal{Q}$ is generated by operators $\varphi_1, \ldots, \varphi_m \in \mathcal{H}_\mathcal{Q}$ and verey $\varphi \in \mathcal{H}_\mathcal{Q}$ can be writen (uniquely, up to the order of the φ_i's) as $\varphi = {\varphi_1}^{c_1} \cdots {\varphi_m}^{c_m}$, where $c_i \in \{0,1\}$. In this case the quantum code $\mathcal{Q}$ has dimension 2^{n-m}. Suppose that $\varphi_i = (-1)^{\lambda_i} X_{\alpha_i} Z_{\beta_i}$. So $\overline{\mathcal{H}_\mathcal{Q}}$ can be determined by its $m \times (2n)$ binary generating matrix

$$M = \left(\begin{array}{c|c} \alpha_1 & \beta_1 \\ \vdots & \vdots \\ \alpha_m & \beta_m \end{array} \right) . \tag{2}$$

Note that if such matrix M obtained from a stabilizer, then $\alpha_i \cdot \beta_i = 0$ and $\alpha_i \cdot \beta_j + \alpha_j \cdot \beta_i = 0$, for every i and j. A quantum code $\mathcal{Q}$ is called *additive* (or *stabilizer*) if it is defined by its stabilizer $\mathcal{H}_\mathcal{Q}$, i.e.,

$$\mathcal{Q} = \left\{ |x\rangle \in \mathbb{C}^{2^n} : \varphi |x\rangle = |x\rangle \text{ for every } \varphi \in \mathcal{H}_\mathcal{Q} \right\} .$$

The quantum codes $\mathcal{Q}_1$ and $\mathcal{Q}_2$ in $\mathbb{C}^{2^n}$ are *locally equivalent* if there is a transversal operator $\mathcal{U} = u_1 \otimes \cdots \otimes u_n$, with $u_i \in \mathrm{SU}(2)$, mapping $\mathcal{Q}_1$ into $\mathcal{Q}_2$. We say these codes are *globally equivalent*, or simply equivalent, if $\mathcal{Q}_1$ is locally equivalent to a code obtained from $\mathcal{Q}_2$ by a permutation on qubits.

A quantum code $\mathcal{Q} \subseteq \mathbb{C}^{2^n}$ is called **nonadditive** if it is not equivalent to any additive code; moreover, $\mathcal{Q}$ is **strongly nonadditive** if the only additive code that contains any code equivalent to $\mathcal{Q}$ is the trivial code $\mathbb{C}^{2^n}$; in other words, if $\pm X_\alpha Z_\beta$ is in the stabilizer of any code equivalent to a supercode of $\mathcal{Q}$ then $\alpha = \beta = \mathbf{0}$.

A K–dimensional subspace of $\mathbb{C}^{2^n}$ that as an error–correcting quantum code can protect against $< d/2$ errors, is called an $((n, K, d))$ code. If This code is additive, then $K = 2^k$, for some k, and it is called an $[[n, k, d]]$ code. The following theorem gives a sufficient condition that a subspace of $\mathbb{C}^{2^n}$ to be an $((n, K, d))$ code. Here $\mathrm{wt}(c)$ denotes the Hamming weight of the binary vector c, i.e. the number of 1–components of c, and $\alpha \cup \beta$ is the binary vector result of componentwise OR operation of α and β; for example $(10110) \cup (00101) = (10111)$.

Theorem 2.1 ([1], [8]) *Let $\mathcal{Q}$ be a K–dimensional subspace of $\mathbb{C}^{2^n}$. Consider an orthonormal basis for $\mathcal{Q}$ of the form $\{\, |c_i\rangle : i = 1, \ldots, K \,\}$. Then $\mathcal{Q}$ is an $((n, K, d))$ code if $\langle c_i \,|\, X_\alpha Z_\beta \,|\, c_j \rangle = 0$ for every $1 \le i, j \le K$ and for every $\alpha, \beta \in \{0, 1\}^n$ with $1 \le \mathrm{wt}(\alpha \cup \beta) \le d - 1$. In general, a necessary and sufficient condition for $\mathcal{Q}$ to be an $((n, K, d))$ code is that for all $1 \le i, j \le K$ and $\mathrm{wt}(\alpha \cup \beta) \le d - 1$ we have $\langle c_i \,|\, X_\alpha Z_\beta \,|\, c_i \rangle = \langle c_j \,|\, X_\alpha Z_\beta \,|\, c_j \rangle$ and if $i \ne j$ then $\langle c_i \,|\, X_\alpha Z_\beta \,|\, c_j \rangle = 0$.*

For an additive code $\mathcal{Q}$ with stabilizer $\mathcal{H}_\mathcal{Q}$ there is a sufficient condition in term of the dual of $\mathcal{H}_\mathcal{Q}$ with respect to the inner product defined by equation (1) for $\mathcal{Q}$ to be a t–error–correcting code.

Theorem 2.2 ([3], [7]) *Let $\mathcal{Q}$ be an additive code with stabilizer $\mathcal{H}_\mathcal{Q}$. Let $\overline{\mathcal{H}_\mathcal{Q}}^{\perp}$ be the space orthogonal to $\overline{\mathcal{H}_\mathcal{Q}}$ with respect to the inner product (1). If for every binary vectors $\alpha, \beta \in \{0, 1\}^n$ with $\mathrm{wt}(\alpha \cup \beta) \le d - 1$ we have $(\alpha|\beta) \notin \overline{\mathcal{H}_\mathcal{Q}}^{\perp} \setminus \overline{\mathcal{H}_\mathcal{Q}}$ then $\mathcal{Q}$ is an $[[n, k, d]]$.*

3 The structure of additive codes

We give a characterization of additive quantum error–correcting codes. Suppose that the matrix M in (2) specifies the stabilizer of an additive code $\mathcal{Q}$. If we add one row of M to another row of it, the resulting matrix also generates $\overline{\mathcal{H}_\mathcal{Q}}$; i.e., the new matrix can be obtained from some other basis of $\mathcal{H}_{\mathcal{Q}}$. So we can assume, without loss of generality, that M has the following structure:

$$M = \left(\begin{array}{c|c} A & B \\ \hline 0 & P \end{array} \right) = \left(\begin{array}{c|c} a_1 & b_1 \\ \vdots & \vdots \\ a_r & b_r \\ \hline 0 & P \end{array} \right), \tag{3}$$

where A and P are full-rank matrices, and A is a generator matrix for the binary code $\mathcal{C}$.

The Calderbank–Shor–Steane (CSS) codes are special class of additive codes with a simple structure. In this section we show that the structure of any additive code is similar to the structure of CSS codes with some differences. Let us first explain the construction of theses codes.

Suppose that $\mathcal{C}$ is a weakly self–dual $[n, k, d_0]$ binary code (i.e., $\mathcal{C} \subseteq \mathcal{C}^{\perp}$). Suppose that $\text{dist}(\mathcal{C}^{\perp}) \geq d$. The vectors $|x_a\rangle = \sum_{c \in \mathcal{C}} |c + a\rangle$, where $a \in \mathcal{C}^{\perp}$, form the CSS code $\mathcal{Q}$. (To simplify the notation, throughout this paper we delete the normalization factors.) Then $\mathcal{Q}$ is an $[[n, n-2k, d]]$ additive code. For $a, a' \in \mathcal{C}^{\perp}$, we have $|x_a\rangle = |x_{a'}\rangle$ if and only if a and a' belong to the same coset of $\mathcal{C}$ in $\mathcal{C}^{\perp}$; so the dimension of $\mathcal{Q}$ is equal to the number of cosets of $\mathcal{C}$ in $\mathcal{C}^{\perp}$, which is 2^{n-2k}.

We show that for any additive code we have a similar basis, but here we have to add some "signs" to the states; i.e., the basis consists of vectors of the form $|x_a\rangle = \sum_{c \in \mathcal{C}} \text{sgn}\,(c + a)\, |c + a\rangle$, where $\mathcal{C}$ is some binary linear code, a's belong to some other linear code (not necessarily $\mathcal{C}^{\perp}$) and $\text{sgn}\,(c + a)$'s are chosen in a very special way from $\{-1, +1\}$ (see equations (9) and (10)). Moreover, we show that these bases characterize additive codes, in the sense that any quantum code that has such a basis (with signs $\text{sgn}\,(c + a)$'s satisfying the equations detemined in the following theorems) is additive.

Theorem 3.1 *Suppose that the 2^{n-m}–dimensional space $\mathcal{Q} \subseteq \mathbb{C}^{2^n}$ is an additive quantum error–correcting code with stabilizer $\mathcal{H}_{\mathcal{Q}}$. Suppose that the full-rank matrix M in* (3) *generates $\overline{\mathcal{H}_{\mathcal{Q}}}$; i.e., $a_i \cdot b_i = 0$ and $a_i \cdot b_j + a_j \cdot b_i = 0$, for all $1 \leq i, j \leq r$, and a_i's belong to the dual space of P. More specifically, let $\mathcal{H}_{\mathcal{Q}}$ be generated by $\{\varphi_1, \ldots, \varphi_m\}$, where $\varphi_i = \varepsilon_i X_{a_i} Z_{b_i}$, for some $\varepsilon_i \in \{-1, +1\}$ and $a_i = \mathbf{0}$ for $r < i \leq m$. Let $\mathcal{C}$ be the the binary linear code generated by $\{a_1, \ldots, a_r\}$. Then there are independent binary vectors $\gamma_1, \ldots, \gamma_{n-m}$ in $\{0, 1\}^n \backslash \mathcal{C}$ generating the linear space Γ such that the followings hold.*

(i) $\mathcal{Q}$ *has a basis consists of the vectors of the form*

$$|x_\gamma\rangle = \sum_{c\in\mathcal{C}} \mathrm{sgn}\,(c+\gamma)\,|c+\gamma\rangle\,, \qquad \gamma\in\Gamma, \tag{4}$$

for some $\mathrm{sgn}\,(c+\gamma)\in\{-1,+1\}$.

(ii) $\mathrm{sgn}\,(c+\gamma)$*'s satisfy the following identities:*

$$\mathrm{sgn}\,(\gamma) = 1 \qquad \textit{for } \gamma\in\Gamma, \tag{5}$$

$$\mathrm{sgn}\,(a_i) = \varepsilon_i \qquad \textit{for } 1\le i\le r, \tag{6}$$

$$\mathrm{sgn}\left(\sum_{j=1}^{\ell} a_{i_j}\right) = (-1)^{b_{i_1}\cdot\sum_{j=2}^{\ell} a_{i_j}}(-1)^{b_{i_2}\cdot\sum_{j=3}^{\ell} a_{i_j}}\cdots(-1)^{b_{i_{\ell-1}}\cdot a_{i_\ell}}\varepsilon_{i_1}\cdots\varepsilon_{i_\ell}, \tag{7}$$

$$\mathrm{sgn}\left(\sum_{j=1}^{\ell} a_{i_j}+\gamma\right) = (-1)^{\gamma\cdot\sum_{j=1}^{\ell} b_{i_j}}\,\mathrm{sgn}\left(\sum_{j=1}^{\ell} a_{i_j}\right), \qquad \textit{for every } \ell\ge 1 \textit{ and } \gamma\in\Gamma. \tag{8}$$

Proof. (i) Let $\mathcal{D}$ be the space of vectors in $\{0,1\}^n$ orthogonal to the rows of P. Then the dimension of $\mathcal{D}$ is $n-m+r$ and $\mathcal{C}\subseteq\mathcal{D}$. Choose vectors $\gamma_1,\ldots,\gamma_{n-m}$ such that $\{a_1,\ldots,a_r,\gamma_1,\ldots,\gamma_{n-m}\}$ be a basis for $\mathcal{D}$. Let Γ be the space generated by $\{\gamma_1,\ldots,\gamma_{n-m}\}$. There are $2^{n-m+r}/2^r = 2^{n-m}$ cosets of $\mathcal{C}$ in $\mathcal{D}$; each coset can be represented as $\gamma+\mathcal{C}$ where $\gamma\in\Gamma$ is a linear combination of γ_j's. It is easy to check that in fact $|x_\gamma\rangle = \sum_{\varphi\in\mathcal{H}_\mathcal{Q}}\varphi\,|\gamma\rangle$, because each operator in $\mathcal{H}_\mathcal{Q}$ can be written as $\pm X_\alpha Z_\beta$, where $\alpha\in\mathcal{C}$ and β is in the group generated by $b_1,\ldots,b_r$ plus the rows of P. So, for every $\psi\in\mathcal{H}_\mathcal{Q}$,

$$\psi\,|x_\gamma\rangle = \sum_{\varphi\in\mathcal{H}_\mathcal{Q}}\psi\varphi\,|\gamma\rangle = \sum_{\varphi\in\mathcal{H}_\mathcal{Q}}\varphi\,|\gamma\rangle = |x_\gamma\rangle\,.$$

Therefore, $|x_\gamma\rangle\in\mathcal{Q}$. On the other hand, $|x_\gamma\rangle$ and $|x_{\gamma'}\rangle$ are orthogonal for $\gamma\neq\gamma'$. So the 2^{n-m} vectors $|x_\gamma\rangle$ form a basis for $\mathcal{Q}$.

(ii) Condition (5) follows form the fact that $I\,|\gamma\rangle = |\gamma\rangle = \mathrm{sgn}\,(\gamma)\,|\gamma\rangle$, and (6) follows from the fact that $\varepsilon_i X_{a_i} Z_{b_i}\,|\mathbf{0}\rangle = \varepsilon_i\,|a_i\rangle$ should be equal to $\mathrm{sgn}\,(a_i)\,|a_i\rangle$.

We can prove (7) by an induction on ℓ. For $\ell=1$, it reduces to (6). Suppose that (7) is true for ℓ. Then (here we are using the fact that $a_i\cdot b_i=0$)

$$\varepsilon_{i_1}X_{a_{i_1}}Z_{b_{i_1}}\,\mathrm{sgn}\left(\sum_{j=1}^{\ell+1} a_{i_j}\right)\left|\sum_{j=1}^{\ell+1} a_{i_j}\right\rangle = \varepsilon_{i_1}(-1)^{b_{i_1}\cdot(\sum_{j=2}^{\ell+1} a_{i_j})}\,\mathrm{sgn}\left(\sum_{j=1}^{\ell+1} a_{i_j}\right)\left|\sum_{j=2}^{\ell+1} a_{i_j}\right\rangle$$

should be equal to

$$\operatorname{sgn}\left(\sum_{j=2}^{\ell+1} a_{i_j}\right)\left|\sum_{j=2}^{\ell+1} a_{i_j}\right\rangle,$$

so it follows

$$\operatorname{sgn}\left(\sum_{j=1}^{\ell+1} a_{i_j}\right) = \varepsilon_{i_1}(-1)^{b_{i_1}\cdot(\sum_{j=2}^{\ell+1} a_{i_j})}\operatorname{sgn}\left(\sum_{j=2}^{\ell+1} a_{i_j}\right).$$

Then the induction hypothesis implies (7).

By a similar inductive argument (8) can be proved. ■

In the next theorem we present relations among $\operatorname{sgn}(c+\gamma)$'s which characterize the additive codes.

Theorem 3.2 *Every sign* $\operatorname{sgn}(c+\gamma)$ *in Theorem* 3.1 *is a function of the following signs*

$$\operatorname{sgn}(a_i)\,,\ \operatorname{sgn}(a_i+a_j)\ \textit{ and }\ \operatorname{sgn}(a_i+\gamma_k) \qquad \textit{for } 1 \le i,j \le r \textit{ and } 1 \le k \le n-m.$$

More specifically, the following relations hold. For every nonempty subsets $S \subseteq \{1,2,\ldots,r\}$ *and* $T \subseteq \{1,2,\ldots,n-m\}$ *we have*

$$\operatorname{sgn}\left(\sum_{i\in S} a_i\right) = \prod_{i\in S}[\operatorname{sgn}(a_i)]^{|S|}\prod_{\substack{i<j\\ i,j\in S}}\operatorname{sgn}(a_i+a_j)\,, \tag{9}$$

$$\operatorname{sgn}\left(\sum_{i\in S} a_i + \sum_{j\in T}\gamma_j\right) = \operatorname{sgn}\left(\sum_{i\in S} a_i\right)\left[\prod_{i\in S}\operatorname{sgn}(a_i)\right]^{|T|}\prod_{\substack{i\in S\\ j\in T}}\operatorname{sgn}(a_i+\gamma_j)\,. \tag{10}$$

Proof. From (6) and (7) it follows

$$(-1)^{b_i\cdot a_j} = \operatorname{sgn}(a_i)\operatorname{sgn}(a_j)\operatorname{sgn}(a_i+a_j)\,. \tag{11}$$

Now (9) follows from (6) and (7) by expanding the inner products and substituting $(-1)^{b_i\cdot a_j}$ from (11).

Similarly, from (8) it follows

$$(-1)^{b_i\cdot\gamma_j} = \operatorname{sgn}(a_i)\operatorname{sgn}(a_i+\gamma_j)\,. \tag{12}$$

Then (8) implies (10). ■

Now we give a characterization of additive codes.

Theorem 3.3 *Let $\mathcal{Q}$, a 2^{n-m}–dimensional subspace of $\mathbb{C}^{2^n}$, be a quantum error–correcting code. Suppose that there is a linear binary code $\mathcal{C} \subseteq \{0,1\}^n$ with basis $\{ a_1, \ldots, a_r \}$, $r \leq m$, and vectors $\gamma_1 \ldots, \gamma_{n-m}$ with the property that $\{ a_1, \ldots, a_r, \gamma_1 \ldots, \gamma_{n-m} \}$ is an indepentdent set (γ_i's are basis for some binary code Γ). Then $\mathcal{Q}$ is an additive code if $\mathcal{Q}$ has a basis $\mathcal{B}$ of the form* (4) *where the signs* $\operatorname{sgn}(c+\gamma)$ *satisfy equations* (5), (9) *and* (10).

Proof. Suppose that $a_1, \ldots, a_r$ is a basis for the binary code $\mathcal{C}$. If $r < m$ then let P be a generator matrix for the linear code that is orthogonal to both $\mathcal{C}$ and Γ. Let $p_1, \ldots, p_{m-r}$ be the rows of P.

For $1 \leq i \leq r$, let $b_i \in \{0,1\}^n$ be any vector that satisfies the equations

$$\begin{aligned} (-1)^{b_i \cdot a_j} &= \operatorname{sgn}(a_i) \operatorname{sgn}(a_j) \operatorname{sgn}(a_i + a_j), \quad 1 \leq j \leq r, \\ (-1)^{b_i \cdot \gamma_j} &= \operatorname{sgn}(a_i) \operatorname{sgn}(a_i + \gamma_j), \quad 1 \leq j \leq n-m. \end{aligned}$$

Such b_i exists, because the above eqautions can be written as a system of $n-m+r$ linear equations with independent vectors a_j's and γ_j's as its coefficient vectors. Consider the group $\mathcal{H}_{\mathcal{Q}}$ of unitary operators generated by

$$e_i = \operatorname{sgn}(a_i) X_{a_i} Z_{b_i}, \quad 1 \leq i \leq r, \quad \text{and} \quad f_i = Z_{p_i}, \quad 1 \leq i \leq m-r.$$

(Of course we consider f_i's only if $r < m$.) Then $\mathcal{H}_{\mathcal{Q}}$ is Abelian: $e_i e_j = e_j e_i$ (for $i \neq j$) follows from the fact that $(-1)^{b_i \cdot a_j} = (-1)^{b_j \cdot a_i} = \operatorname{sgn}(a_i) \operatorname{sgn}(a_j) \operatorname{sgn}(a_i + a_j)$; $e_i f_j = f_j e_i$ and $f_i f_j = f_j f_i$ are obvious. Also every element of $\mathcal{H}_{\mathcal{Q}}$ sqaures to identity: $e_i{}^2 = I$ follows from the fact that $(-1)^{a_i \cdot b_i} = \operatorname{sgn}(a_i) \operatorname{sgn}(a_i) \operatorname{sgn}(a_i + a_i) = 1$ so $a_i \cdot b_i = 0$; $f_i{}^2 = I$ is obvious. Thus $\mathcal{H}_{\mathcal{Q}}$ is the stabilizer of an additive quantum code $\mathcal{Q}'$ of dimension 2^{n-m}. Consider the basis $\mathcal{B}'$ for $\mathcal{Q}'$ provided by Theorem 3.1. Then, by Theorem 3.2, $\mathcal{B} = \mathcal{B}'$. So $\mathcal{Q} = \mathcal{Q}'$, and $\mathcal{Q}$ is an additive code. ■

4 Existence of nonadditive codes

4.1 Quantum codes equivalent to additive codes

We study the quantum codes equivalent to additive codes. For such code $\mathcal{Q}$, we find a sufficient condition that guarantees that the stabilizer of $\mathcal{Q}$ contains a nontrivial operator.

We begin with some useful notions and notations. Let $|c_1\rangle, \ldots, |c_{2^n}\rangle$ be the standard orthonormal basis of $\mathbb{C}^{2^n}$, where each c_i is a binary vector of length n. For the vector

$|x\rangle = \sum_{i=1}^{2^n} \lambda_i |c_i\rangle$, we define the *support* of $|x\rangle$ as

$$\mathrm{supp}(|x\rangle) = \{\, c_i \in \{0,1\}^n : \lambda_i \neq 0 \,\}\,.$$

Let $\mathcal{C} \subseteq \{0,1\}^n$ be a set of binary vectors. Define the vector $|\mathcal{C}\rangle$ in $\mathbb{C}^{2^n}$ as

$$|\mathcal{C}\rangle = \frac{1}{|\mathcal{C}|^{1/2}} \sum_{c \in \mathcal{C}} |c\rangle\,.$$

(If $\mathcal{C}$ is empty then $|\mathcal{C}\rangle$ is the zero vector.) For any binary vector α of length $m < n$, define

$$\mathcal{C}_\alpha = \left\{\, x \in \{0,1\}^{n-m} : (\alpha, x) \in \mathcal{C} \,\right\}. \tag{13}$$

So to construct $\mathcal{C}_\alpha$, consider all vectors in $\mathcal{C}$ starting with α (if there is any), then delete α from these vectors. Note that $\mathcal{C}_\alpha$ may be empty.

For a quantum code $\mathcal{Q}$, let us define *the generalized stabilizer* of $\mathcal{Q}$ as the set $GS(\mathcal{Q})$ of all unitary operators $\mathcal{V}$ on $\mathbb{C}^{2^n}$ such that $\mathcal{V}|x\rangle = |x\rangle$ for every $|x\rangle \in \mathcal{Q}$. Then the *stabilizer* of $\mathcal{Q}$ is $\mathrm{St}(\mathcal{Q}) = \mathcal{G} \cap GS(\mathcal{Q})$.

Lemma 4.1 *Suppose that the quantum codes $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are locally equivalent via the transversal unitary operator $\mathcal{U}$. Then for every $M \in GS(\mathcal{Q}_1)$ the operator $\mathcal{U}M\mathcal{U}^\dagger$ is in $GS(\mathcal{Q}_2)$.*

Proof. Let $|x\rangle \in \mathcal{Q}_2$. There is $|y\rangle \in \mathcal{Q}_1$ such that $|x\rangle = \mathcal{U}|y\rangle$. Since $M|y\rangle = |y\rangle$, so $(M\mathcal{U}^\dagger)\mathcal{U}|y\rangle = |y\rangle$, and therefore $(\mathcal{U}M\mathcal{U}^\dagger)\mathcal{U}|y\rangle = \mathcal{U}|y\rangle$. This implies $(\mathcal{U}M\mathcal{U}^\dagger)|x\rangle = |x\rangle$. ■

We are interested in the case of $M \in \mathcal{G}$, i.e., $M = M_1 \otimes \cdots \otimes M_n$, where $M_j \in \{I, \sigma_x, \sigma_y, \sigma_z\}$. We define $\mathrm{wt}(M)$ the *weight* of any $M \in \mathcal{G}$ as the number of j's such that $M_j \neq I$. In this case $\mathcal{U}M\mathcal{U}^\dagger = v_1 \otimes \cdots \otimes v_n$ such that $\det(v_j) = \pm 1$ and if $M_j = I$ then $v_j = I$, otherwise

$$v_j = \eta_j \begin{pmatrix} a_j & b_j \\ \pm {b_j}^* & -a_j \end{pmatrix}, \qquad \eta_j \in \{1, i\},\ a_j \in \mathbb{R} \text{ and } b_j \in \mathbb{C}. \tag{14}$$

If $\mathcal{U} \in \mathrm{SU}(2)^{\otimes n}$ then $\mathcal{U}$ is of the form $u_1 \otimes \cdots \otimes u_n$, where each u_j is defined by a matrix of the form

$$\begin{pmatrix} e^{i\alpha}\cos\theta & e^{i\beta}\sin\theta \\ -e^{-i\beta}\sin\theta & e^{-i\alpha}\cos\theta \end{pmatrix}. \tag{15}$$

If $M_j = \sigma_x$, σ_z or σ_y, then the corresponding v_j, repectively, is

$$\left.\begin{array}{r}\begin{pmatrix} \sin 2\theta\cos(\alpha-\beta) & \cos^2\theta e^{i2\alpha} - \sin^2\theta e^{i2\beta} \\ \cos^2\theta e^{-i2\alpha} - \sin^2\theta e^{-i2\beta} & -\sin 2\theta\cos(\alpha-\beta) \end{pmatrix}, \\ \\ \begin{pmatrix} \cos 2\theta & -\sin 2\theta e^{i(\alpha+\beta)} \\ -\sin 2\theta e^{-i(\alpha+\beta)} & -\cos 2\theta \end{pmatrix}, \\ \\ \text{or } \begin{pmatrix} -i\sin 2\theta\sin(\alpha-\beta) & -\cos^2\theta e^{i2\alpha} - \sin^2\theta e^{i2\beta} \\ \cos^2\theta e^{-i2\alpha} + \sin^2\theta e^{-i2\beta} & i\sin 2\theta\sin(\alpha-\beta) \end{pmatrix}. \end{array}\right\} \tag{16}$$

We call a matrix v_i as (14) *full* if $a_i \cdot b_i \neq 0$; and we say the unitary operator $\mathcal{V} = v_1 \otimes \cdots \otimes v_n$ is *thin* if none of v_i's is full. In the next proof we will use this property that if $\mathcal{V}$ is thin then $|\text{supp}(\mathcal{V}\,|x\rangle)| = |\text{supp}(|x\rangle)|$, for every $|x\rangle$.

A quantum code $\mathcal{Q}$ is called *real* if $\mathcal{Q}$ has a basis consisting of real vectors; i.e., if $|x\rangle = \sum_{i=1}^{2^n} \lambda_i\,|c_i\rangle$ is any vector in the basis, then $\lambda_i \in \mathbb{R}$, for every i.

An (n, K, d) binary code is a set $\mathcal{C} \subseteq \{0,1\}^n$ of size K such that any two vectors in $\mathcal{C}$ differ in at least d places, and d is the largest number with this property. Note that an $[n, k, d]$ binary linear code is an $(n, 2^k, d)$ binary code.

Theorem 4.2 *Suppose that the quantum codes $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are locally equivalent via the transversal operator $\mathcal{U}$, $\mathcal{Q}_2$ is real and $\mathcal{Q}_2$ contains $|\mathcal{C}\rangle$, where $\mathcal{C}$ is an (n, K, d) binary code with $d > k = \lceil \log_2 K \rceil$. Then the following claims hold.*

(i) The image of $\text{St}(\mathcal{Q}_1)$ *under the mapping $M \mapsto \mathcal{U}M\mathcal{U}^\dagger$, which we call Γ, consists only of unitary operators $\pm X_\alpha T$, where T is a Z–type unitary operator of the form*

$$T = \bigotimes_{j=1}^{n} \begin{pmatrix} e^{i\theta_j} & 0 \\ 0 & \pm e^{-i\theta_j} \end{pmatrix}. \tag{17}$$

(ii) Let $\Delta = \{\, \alpha \in \{0,1\}^n : \pm X_\alpha T \in \Gamma \text{ for some } T \text{ of the form (17)} \,\}$. *Suppose that* $\text{St}(\mathcal{Q}_2)$ *does not contain any operator of the form $\pm X_{\mathbf{0}} Z_\beta$, with $\beta \neq \mathbf{0}$. Then* $|\text{St}(\mathcal{Q}_1)| \leq |\Delta|$.

Proof. By Lemma 4.1, there are $v_i \in \text{SU}(2)$, $1 \leq i \leq n$, such that $v_i = I$ or v_i satisfies (14) (or, equivalently (16)) and for $\mathcal{V} = v_1 \otimes \cdots \otimes v_n$ we have

$$\mathcal{V}\,|\mathcal{C}\rangle = |\mathcal{C}\rangle\,, \tag{18}$$

We claim $\mathcal{V}$ is a thin operator. By contradiction, assume $\mathcal{V}$ is not thin; and, w.l.o.g., v_1 is full. Let $\mathcal{V}_1 = v_2 \otimes \cdots \otimes v_n$. Define $\mathcal{C}_0$ and $\mathcal{C}_1$ as (13), i.e.,

$$\mathcal{C}_0 = \left\{ x \in \{0,1\}^{n-1} : (0,x) \in \mathcal{C} \right\},$$

and a similar eqaution for $\mathcal{C}_1$. Thus, $|\mathcal{C}\rangle = |0\rangle \otimes |\mathcal{C}_0\rangle + |1\rangle \otimes |\mathcal{C}_1\rangle$. Then (18) implies

$$\begin{aligned} a_1 \mathcal{V}_1 |\mathcal{C}_0\rangle \pm {b_1}^* \mathcal{V}_1 |\mathcal{C}_1\rangle &= |\mathcal{C}_0\rangle, \\ b_1 \mathcal{V}_1 |\mathcal{C}_0\rangle - a_1 \mathcal{V}_1 |\mathcal{C}_1\rangle &= |\mathcal{C}_1\rangle. \end{aligned}$$

This shows that $\mathcal{C}_0$ and $\mathcal{C}_1$ both should be non–empty. By solving this system, we get

$$\begin{aligned} \mathcal{V}_1 |\mathcal{C}_0\rangle &= -a_1 |\mathcal{C}_0\rangle \mp {b_1}^* |\mathcal{C}_1\rangle, \\ \mathcal{V}_1 |\mathcal{C}_1\rangle &= -b_1 |\mathcal{C}_0\rangle + a_1 |\mathcal{C}_1\rangle. \end{aligned}$$

If $\mathcal{V}_1$ is thin then $|\text{supp}(|\mathcal{C}_0\rangle)| = |\text{supp}(|\mathcal{C}_0\rangle)|$, but since $\text{supp}(|\mathcal{C}_0\rangle) \cap \text{supp}(|\mathcal{C}_1\rangle) = \emptyset$, it follows that $\mathcal{V}_1$ is not thin and for some i, $2 \le i \le n$, v_i should be a full matrix. Assume, w.l.o.g., v_2 is full. Then, with a similar calculation for $\mathcal{V}_2 = v_3 \otimes \cdots \otimes v_n$,

$$\mathcal{V}_2 |\mathcal{C}_{\alpha_i}\rangle = \sum_{j=1}^{4} \lambda_j \left|\mathcal{C}_{\alpha_j}\right\rangle, \qquad 1 \le i \le 4,$$

where α_i is a binary vector of length 2 and each λ_j is a product of entries of v_1 and v_2 (so each λ_j is nonzero). If $K \ge 4$, then $\text{supp}(|\mathcal{C}_{\alpha_i}\rangle)$ are disjoint (because $d > k$) and they should be non–empty. Therefore, at least one of $v_3, \ldots, v_n$ should be full. Again, w.l.o.g., we acn assume v_3 is full. By continuing this argument, we find out that k of v_i's, say $v_1, \ldots, v_k$, are full and for $\mathcal{V}_k = v_{k+1} \otimes \cdots \otimes v_n$ and any $\beta \in \{0,1\}^k$ we have

$$\mathcal{V}_k |\mathcal{C}_\beta\rangle = \sum_{\alpha \in \{0,1\}^k} \lambda_\alpha |\mathcal{C}_\alpha\rangle, \tag{19}$$

where each λ_α is a product of the entries of $v_1, \ldots, v_k$, so all λ_α are nonzero. Since $d > k$, all $\mathcal{C}_\alpha$, $\alpha \in \{0,1\}^k$, have disjoint support. Therefore, for every $\alpha \in \{0,1\}^k$, $\mathcal{V}_k |\mathcal{C}_\alpha\rangle \neq 0$. This implies that for every α, the size of $\text{supp}(|\mathcal{C}_\alpha\rangle)$ is one. Therefore, for every $\alpha \in \{0,1\}^k$, either $|\mathcal{C}_{\alpha 0}\rangle = 0$ or $|\mathcal{C}_{\alpha 1}\rangle = 0$ We conclude that $\mathcal{V}_k$ can not be thin, so at least one of $v_{k+1}, \ldots, v_n$ is full. Suppose that v_{k+1} is full and let $\mathcal{V}_{k+1} = v_{k+2} \otimes \cdots \otimes v_n$. Consider any $\beta \in \{0,1\}^k$. Then either $\text{supp}(|\mathcal{C}_{\beta 0}\rangle) = \emptyset$ or $\text{supp}(|\mathcal{C}_{\beta 1}\rangle) = \emptyset$. Assume, w.l.o.g., that $\text{supp}(|\mathcal{C}_{\beta 1}\rangle) = \emptyset$. Therefore, $|\mathcal{C}_\beta\rangle = |0\rangle \otimes |\mathcal{C}_{\beta 0}\rangle$. Then (19) implies

$$a_{k+1} |0\rangle \otimes \mathcal{V}_{k+1} |\mathcal{C}_{\beta 0}\rangle + b_{k+1} |1\rangle \otimes \mathcal{V}_{k+1} |\mathcal{C}_{\beta 0}\rangle = |0\rangle \otimes \sum_{\alpha \in \{0,1\}^k} \lambda_\alpha |\mathcal{C}_{\alpha 0}\rangle + |1\rangle \otimes \sum_{\alpha \in \{0,1\}^k} \lambda_\alpha |\mathcal{C}_{\alpha 1}\rangle.$$

Thus

$$\mathcal{V}_{k+1}\left|\mathcal{C}_{\beta 0}\right\rangle = \frac{1}{a_{k+1}} \sum_{\alpha\in\{0,1\}^k} \lambda_\alpha \left|\mathcal{C}_{\alpha 0}\right\rangle = \frac{1}{b_{k+1}} \sum_{\alpha\in\{0,1\}^k} \lambda_\alpha \left|\mathcal{C}_{\alpha 1}\right\rangle .$$

Therefre

$$\frac{1}{a_{k+1}} \sum_{\alpha\in\{0,1\}^k} \lambda_\alpha \left|\mathcal{C}_{\alpha 0}\right\rangle - \frac{1}{b_{k+1}} \sum_{\alpha\in\{0,1\}^k} \lambda_\alpha \left|\mathcal{C}_{\alpha 1}\right\rangle = 0.$$

Which is not possible, because in this equation 2^k vectors are zero and the other 2^k vectors are linearly independent and all coefficients are nonzero.

Now to see that the statement (i) of the theorem holds, it is enough to note that

$$\begin{pmatrix} 0 & e^{i\theta} \\ \pm e^{-i\theta} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \pm e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}.$$

Now we are ready to prove (ii). Suppose that $X_{\alpha_1}Z_{\beta_1}$ and $X_{\alpha_2}Z_{\beta_2}$ are in $\mathrm{St}(\mathcal{Q}_1)$ and $(\alpha_1,\beta_1)\neq(\alpha_2,\beta_2)$. Suppose that $X_{\alpha_j}Z_{\beta_j}$ is mapped to $\mathcal{V}_j = \pm v_1^j\otimes\cdots\otimes v_n^j$, $j=1,2$, where each v_l^j is of the form (14), or more explicitly of the form (16). Let $\mathcal{V}_j = X_{a_j}T_j$, $j=1,2$. We assume $a_1=a_2=a$ and derive a contradiction. Without loss of generality, we can assume $a = (\overbrace{1,\ldots,1}^{m \text{ times}},0,\ldots,0)$. Therefore, $v_\ell^1 = v_\ell^2 = \{I,\sigma_z\}$, for $\ell = m+1,\ldots,n$; and the matrix of v_ℓ^j, $j=1,2$ and $\ell=1,\ldots,m$, is anti–diagonal, i.e., it is of the form $\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$.

Before we continue note that the matrices of $v_x = u\sigma_x u^\dagger$, $v_y = u\sigma_y u^\dagger$, $v_z = u\sigma_z u^\dagger$, for a fixed $u\in\mathrm{SU}(2)$, are of the form (16), and if two of $\{\, v_x, v_y, v_z \,\}$ are anti–diagonal then the third is diagonal, and if one of them is diagonal then the other two are anti–diagonal.

Now we show that the operator $X_{\alpha_1+\alpha_2}Z_{\beta_1+\beta_2}$ in $\mathrm{St}(\mathcal{Q}_1)$ is mapped to an operator $v_1\otimes\cdots\otimes v_n$ of the form $X_{\mathbf{0}}Z_\beta$ with $\beta\neq\mathbf{0}$, which is the desired contradiction. Note that if $v_\ell^j = u_\ell\sigma^j u_\ell^\dagger$, for $j=1,2$ and $\sigma^j\in\{I,\sigma_x,\sigma_y,\sigma_z\}$, then $v_\ell = u_\ell\sigma^1\sigma^2u_\ell^\dagger$. For $\ell = m+1,\ldots,n$, since v_ℓ^1 and v_ℓ^2 both have diagonal matrices, then either σ^1 and σ^2 are identical or one of them is the identity operator. In either case $v_\ell = I$ or σ_z. Similarly, for $i=1,\ldots,m$, v_ℓ^1 and v_ℓ^2 both have anti–diagonal matrices and v_ℓ should be either identity or σ_z. This shows that $v_1\otimes\cdots\otimes v_n = X_{\mathbf{0}}Z_\beta$. It remains to show that at least one of v_ℓ is not identity. Since $(\alpha_1+\alpha_2 \mid \beta_1+\beta_2)\neq\mathbf{0}$, at least one of v_ℓ is of the form $u_l\sigma u_i^\dagger$, where $\sigma\in\{\sigma_x,\sigma_y,\sigma_z\}$. So the matrix of v_ℓ is of the form (16) which is never an identity matrix. ■

We now present a criterion for nonadditiveness of quantum codes. First a useful notation. For a subset $\mathcal{C}$ of $\{0,1\}^n$ let

$$\mathcal{T}(\mathcal{C}) = \{\, x\in\{0,1\}^n : x+\mathcal{C}\subseteq\mathcal{C} \,\}.$$

If $\mathcal{C}$ is a binary *linear* code then $\mathcal{T}(\mathcal{C}) = \mathcal{C}$.

Theorem 4.3 *Suppose that the quantum code $\mathcal{Q}$ of dimension 2^ℓ is real and contains $|\mathcal{C}\rangle$, where $\mathcal{C}$ is an (n, K, d) binary code with $d > \lceil \log_2 K \rceil$. If the identity operator is the only unitary operator in the stabilizer of $\mathcal{Q}$ and $2^{n-\ell} > |\mathcal{T}(\mathcal{C})|$ then $\mathcal{Q}$ is nonadditive.*

Proof. Suppose, by contradiction, that $\mathcal{Q}$ is equivalent to additive code $\mathcal{Q}'$ via the transversal unitary operator $\mathcal{U}$ which mapps $\mathcal{Q}'$ on $\mathcal{Q}$. Let Γ be the image of $\mathrm{St}(\mathcal{Q}')$ under $\mathcal{U}$. Define $\Delta \subseteq \{0,1\}^n$ as in (ii) of Theorem 4.2. Then $\Delta \subseteq \mathcal{T}(\mathcal{C})$. Thus

$$2^{n-\ell} = |\mathrm{St}(\mathcal{Q}')| \leq |\Delta| \leq |\mathcal{T}(\mathcal{C})|,$$

which contradicts the assumption of the theorem. ■

When the binary code $\mathcal{C}$ in the above theorem is linear we can formulate the theorem as follows.

Corollary 4.4 *Suppose that the quantum code $\mathcal{Q}$ of dimension 2^ℓ is real and contains $|\mathcal{C}\rangle$, where $\mathcal{C}$ is a linear $[n, k, d]$ code with $d > k$. If $\mathrm{St}(\mathcal{Q}) = \{I\}$ and $n > k + \ell$ then $\mathcal{Q}$ is nonadditive.*

Finally, we fomulate a criterion that guarantees strongly nonadditiveness of quantum codes.

Theorem 4.5 *Suppose that the qauntum code $\mathcal{Q}$ is real and it contains $|\mathcal{C}\rangle$ where $\mathcal{C}$ is an (n, K, d) binary code with $d > \lceil \log_2 K \rceil$. If $\mathrm{St}(\mathcal{Q}) = \{I\}$ and $GS(\mathcal{Q})$ does not contain any operator of the form $X_\alpha T$, where $\alpha \neq \mathbf{0}$ and T is of the form (17), then $\mathcal{Q}$ is strongly nonadditive.*

Proof. Suppose, by contradiction, that $\mathcal{Q} \subseteq \mathcal{Q}_1$ and $\mathcal{Q}_1 \neq \mathbb{C}^{2^n}$ is equivalent to an additive code $\mathcal{Q}'$ with $\mathrm{St}(\mathcal{Q}') \neq \{I\}$. Then, by Theorem 4.2, any nontrivial stabilizer φ of $\mathcal{Q}'$ defines an operator $\mathcal{V} = v_1 \otimes \cdots \otimes v_n$ in $GS(\mathcal{Q}_1) \subseteq GS(\mathcal{Q})$, where $v_j = I$ or it is of the form (14) or (16). If all v_j have real matrices, then $\mathcal{V} \neq I$ and $\mathcal{V} \in \mathrm{St}(\mathcal{Q})$, which is impossible. If at least one of v_j has a complex matrix, then $\mathcal{V}$ is of the form $X_\alpha T$ with $\alpha \neq \mathbf{0}$, which is again impossible. ■

4.2 Construction of nonadditive codes

4.2.1 Examples of nonadditive codes

Now we show that there is an infinite family of nonadditive quantum error–correcting codes. These codes are constructed following the scheme similar to the one described in Theorem 2.4 of [15]. Consider an $[n,k]$ binary code $\mathcal{C}$ such that $\text{dist}(\mathcal{C})$ and $\text{dist}(\mathcal{C}^\perp)$ are both at least d_0 ($\mathcal{C}$ needs not to be a weakly self–dual code).

First we define a function $\tau : \mathcal{C} \longrightarrow \{0,1\}^n$ such that for $c, c' \in \mathcal{C}$ and $c \neq c'$ we have $\tau(c) + \tau(c') \notin \mathcal{C}^\perp$. This means $\tau(c)$ and $\tau(c')$ are in different cosets of $\mathcal{C}^\perp$ in $\{0,1\}^n$, for $c \neq c'$. Since there are 2^k different cosets, such mapping τ always can be defined.

Fix $d \leq d_0$, and let $\mathcal{E}$ be the set of binary vectors of length n with weight $\leq d-1$. Consider a subset $R = \{\, a_0, a_1, \ldots, a_m \,\}$ of $\{0,1\}^n$ such that $a_0 = \mathbf{0}$ and a_j is not of the form $c + a_i + e$, for $c \in \mathcal{C}$, $1 \leq i \leq j-1$, and $e \in \mathcal{E}$. Then the vectors

$$|x_i\rangle = \sum_{c\in\mathcal{C}} (-1)^{\tau(c)\cdot a_i} \, |c + a_i\rangle \tag{20}$$

form a basis for a quantum code with distance d. To prove this, we show that $\langle x_i \mid X_\alpha Z_\beta \mid x_j\rangle = 0$, for $0 < \text{wt}(\alpha \cup \beta) < d$. The case $\alpha \neq \mathbf{0}$ or $i \neq j$ is straightforward. So we only consider the case $\alpha = \mathbf{0}$ and $i = j$. Then for $0 < \text{wt}(\beta) < d$ we have

$$\begin{aligned}
\langle x_i \mid Z_\beta \mid x_i\rangle &= \left\langle \sum_{c\in\mathcal{C}} (-1)^{\tau(c)\cdot a_i} \, |c + a_i\rangle \,\middle|\, \sum_{c\in\mathcal{C}} (-1)^{\tau(c)\cdot a_i + (c+a_i)\cdot\beta} \, |c + a_i\rangle \right\rangle \\
&= (-1)^{a_i\cdot\beta} \sum_{c\in\mathcal{C}} (-1)^{c\cdot\beta} \\
&= 0.
\end{aligned}$$

The last equality follows from the fact that $\text{dist}(\mathcal{C}^\perp) \geq d$, so $\beta \notin \mathcal{C}^\perp$.

Lemma 4.6 *In the above construction, suppose that*

$$(n-1)2^k \sum_{i=0}^{d-1} \binom{n}{i} < 2^{n-1}. \tag{21}$$

Then it is possible to choose n linearly independent vectors $a_1, a_2, \ldots, a_n$ so that the $((\,n, n+1, d\,))$ quantum code $\mathcal{Q}$ with the basis $|x_0\rangle, |x_1\rangle, \ldots, |x_n\rangle$ (each $|x_i\rangle$ is defined by (20)*) has trivial stabilizer, i.e.,* $\text{St}(\mathcal{Q}) = \{I\}$.

Proof. Suppose that the vectors $a_0, a_1, \ldots, a_m$ with the desired properties are chosen. Then it is possible to choose a vector a_{m+1} such that $a_1, \ldots, a_m, a_{m+1}$ are independent and a_{m+1} is not of the form $c+a_i+e$ (for $c \in \mathcal{C}$, $1 \leq i \leq m$, and $e \in \mathcal{E}$) if $2^m+m\cdot 2^k \cdot \sum_{i=0}^{d-1} \binom{n}{i} < 2^n$. This shows that it is possible to choose n vector $a_1, \ldots, a_n$ with the desired properties.

Now we show that the identity operator is the only member of the stabilizer of $\mathcal{Q}$. Suppose that $X_\alpha Z_\beta$ is in the stabilizer of $\mathcal{Q}$. Since

$$X_\alpha Z_\beta \left|x_0\right\rangle = \sum_{c\in\mathcal{C}} (-1)^{c\cdot\beta} \left|c+\alpha\right\rangle$$

should be equal to $\left|x_0\right\rangle = \sum_{c\in\mathcal{C}} \left|c\right\rangle$ it follows that $\alpha \in \mathcal{C}$ and $\beta \in \mathcal{C}^\perp$. Similarly, for every $1 \leq i \leq n$ since

$$\begin{aligned} X_\alpha Z_\beta \left|x_i\right\rangle &= \sum_{c\in\mathcal{C}} (-1)^{\tau(c)\cdot a_i+(c+a_i)\cdot\beta} \left|c+a_i+\alpha\right\rangle \\ &= \sum_{c\in\mathcal{C}} (-1)^{\tau(c+\alpha)\cdot a_i+(c+a_i+\alpha)\cdot\beta} \left|c+a_i\right\rangle \\ &= \sum_{c\in\mathcal{C}} (-1)^{(\tau(c+\alpha)+\beta)\cdot a_i} \left|c+a_i\right\rangle \end{aligned}$$

should be equal to

$$\left|x_i\right\rangle = \sum_{c\in\mathcal{C}} (-1)^{\tau(c)\cdot a_i} \left|c+a_i\right\rangle,$$

it follows that $a_i \cdot (\tau(c)+\tau(c+\alpha)+\beta) = 0$, for every $1 \leq i \leq n$. Since a_i's are independent, therefore $\tau(c)+\tau(c+\alpha) = \beta \in \mathcal{C}^\perp$, hence $\alpha = \mathbf{0}$. Now the conditions $a_i \cdot \beta = 0$ (for $1 \leq i \leq n$) imply $\beta = \mathbf{0}$. ■

Theorem 4.7 *Suppose that $\mathcal{C}$ is an $[n,k,d_0]$ binary linear code such that $d_0 > k$ and dist($\mathcal{C}$) and dist($\mathcal{C}^\perp$) are at least d. Morover, suppose that n, k and d satisfy* (21)*. Let ℓ be the greatest integer such that $2^\ell \leq 2^{n-k}/\sum_{i=0}^{d-1}\binom{n}{i}$. Suppose that $k+\ell < n$. Then there is a an $((n, 2^\ell, d))$ nonadditive code.*

Proof. Consider the $((n, n+1, d))$ code $\mathcal{Q}_0$ constructed in the previous lemma. Then by Theorem 4.2 of [15] it is possible to add at least $2^\ell - (n+1)$ more vectors to $\mathcal{Q}_0$ to build an $((n, 2^\ell, d))$ code $\mathcal{Q}$, which is, by Corollary 4.4, nonadditive. ■

As an application we show that there are $((n, \lfloor 2^{n-1}/(n+1) \rfloor, 2))$ nonadditive codes, for every $n \geq 8$. Consider the $[n, 1, n]$ binary code $\mathcal{C} = \{\mathbf{0}, \mathbf{1}\}$. Then $\mathcal{C}^{\perp}$ is consists of all even weight vectors in $\{0, 1\}^n$, so it is an $[n, n-1, 2]$ code. The condition (21) satisfies if $n \geq 8$. Then by applying the above theorem (for $k = 1$ and $\ell = \lceil n - 1 - \log_2(n+1) \rceil$) we get the desired code. Other classes of binary codes for which the minimum distance of the code and its dual are known (such as Hamming codes and Reed–Muller codes) can be used to get nonadditive codes with different parameters.

Finally, we show that the nonadditive codes are almost as good as Calderbank–Shor–Steane (CSS) codes, at least in the case that the dimension of code is large enough. The construction of CSS codes was explained in the beginning of Section 3.

To utilize the CSS codes for constructing nonadditive codes, we must modify them such that the new codes have trivial stabilizer. Let $\mathcal{Q}$ be an $[[n, n-2k, d]]$ CCS code based on the weakly self–dual $[n, k]$ code $\mathcal{C}$ with $\operatorname{dist}(\mathcal{C}^{\perp}) \geq d$. Consider the basis for $\mathcal{Q}$ consists of vectors $|x_a\rangle = \sum_{c \in \mathcal{C}} |c + a\rangle$, for $a \in \mathcal{C}^{\perp}/\mathcal{C}$. Also consider the function $\tau \colon \mathcal{C} \longrightarrow \{0, 1\}^n$ defined at the beginning of this section. We define the quantum code $\widehat{\mathcal{Q}}$ with basis

$$|y_a\rangle = \sum_{c \in \mathcal{C}} (-1)^{\tau(c) \cdot a} |c + a\rangle\,, \tag{22}$$

for $a \in \mathcal{C}^{\perp}/\mathcal{C}$. Then it is easy to check that $\widehat{\mathcal{Q}}$ is also an $[[n, n-2k, d]]$ code.

Theorem 4.8 *Suppose that $\mathcal{C}$ is an $[n, k, d_0]$ weakly self–dual binary code, and $\mathcal{C}^{\perp}$ is an $[n, n-k, d_1]$ code. Assume $d_0 \geq k$ and $2^{n-2k-1} > n - k - 1$ (for example it is enough that $k < (n - \log_2 n)/2$). For any $d \leq d_1$ that staisfies*

$$\left(2^{n-k} + (k-1)2^k\right) \sum_{i=0}^{d-1} \binom{n}{i} < 2^{n-1}, \tag{23}$$

we have an $((n, 2^{n-2k}, d))$ nonadditive code.

Proof. Let $\mathcal{Q}_0$ be the $[[n, n-2k, d]]$ CSS code based on $\mathcal{C}$, and let $\widehat{\mathcal{Q}_0}$ be the quantum code obtained from $\mathcal{Q}_0$ as described in the above. We can choose independent vectors $a_1, \ldots, a_{n-k}$ in $\mathcal{C}^{\perp}$ such that a_i's belong to different cosets of $\mathcal{C}$ in $\mathcal{C}^{\perp}$. This is possible because $2^{n-2k-1} > n - k - 1$. We consider $|y_{a_1}\rangle, \ldots, |y_{a_{n-k}}\rangle$ (defined by (22)) as vectors in $\widehat{\mathcal{Q}_0}$. Then we choose vectors $a_{n-k+1}, \ldots, a_n$ such that $a_1, \ldots, a_n$ are n independent vectors, and $\mathcal{Q}' = \widehat{\mathcal{Q}_0} \cup \left\{|x_{a_{n-k+1}}\rangle, \ldots, |x_{a_n}\rangle\right\}$, is an $((n, 2^{n-2k} + k, d))$ code. The inequality (23) implies that it is possible to choose $a_{n-k+1}, \ldots, a_n$ with the desired properties. Then the proof of Lemma 4.6 shows that $\mathrm{St}(\mathcal{Q}') = \{I\}$

Let $\mathcal{Q}$ be the quantum code obtained from $\mathcal{Q}'$ by removing any k vectors except $|y_{a_i}\rangle$, $i = 1, \ldots, n$. Then $\mathrm{St}(\mathcal{Q}) = \{I\}$ (because $\mathcal{Q}$ contains the $|y_{a_i}\rangle$, $i = 1, \ldots, n$). So, by Corollary 4.4 with $\ell = n - 2k$, $\mathcal{Q}$ is nonadditive. ■

To show that there are weakly self–dual codes $\mathcal{C}$ that satisfy the requirements of the above theorem, apply the greedy method used in classical coding theory (see [10], Chap. 17). The same method is used in [5] to prove the existence of CSS codes meeting the Gilbert–Varshamov bound.

Suppose that n is even. Let $\Phi_{n,k}$ be the set of all $[n, k]$ weakly self–dual codes; and $\Phi'_{n,k}$ be the set of all codes $\mathcal{C}^\perp$ where $\mathcal{C}$ is in $\Phi_{n,k}$. Let $\varphi = |\Phi_{n,k}| = |\Phi'_{n,k}|$. In [9] (see also [10] p. 630) it is shown that every *nonzero* vector v with even weight belongs to exactly $\sigma_{n,k}$ codes in $\Phi_{n,k}$, where the number $\sigma_{n,k}$ does not depend on the vector v. It is also shown in [5] that every even–weight vector $v \notin \{\mathbf{0}, \mathbf{1}\}$ belongs to exaclty $\sigma'_{n,k}$ codes in $\Phi'_{n,k}$. Then

$$\begin{aligned} \left(2^{n-1} - 1\right) \sigma_{n,k} &= \left(2^k - 1\right) \varphi, \\ \left(2^{n-1} - 2\right) \sigma'_{n,k} &= \left(2^{n-k} - 2\right) \varphi. \end{aligned}$$

Then the number of codes in $\Phi'_{n,k}$ with minimum distance $\leq d$ is at most

$$\begin{aligned} \sum_{j=0}^{d} \binom{n}{j} \sigma'_{n,k} &\leq 2^{H_2(d/n)n} \sigma'_{n,k} \\ &\leq 2^{H_2(d/n)n-k+1} \varphi, \end{aligned}$$

where H_2 is the binary entropy function $H_2(t) = -t \log_2 t - (1-t)\log_2(1-t)$. Let $k = \lceil H_2(d/n)n \rceil + 3$, then more than $\frac{3}{4}$ of the codes in $\Phi'_{n,k}$ have minimum distance greater than d. Now in the class $\Phi_{n,k}$, for the value of d_1 such that $k \leq d_1$ and $k \leq n - H_2(d_1/n)n - 2$, it follows that at most half of the codes in $\Phi_{n,k}$ have minimum distance $\leq d_1$; because the number of codes in $\Phi_{n,k}$ that contain a codeword of weight $< d_1$ is at most

$$\begin{aligned} \sum_{j=0}^{d_1} \binom{n}{j} \sigma_{n,k} &\leq 2^{H_2(d_1/n)n} \sigma_{n,k} \\ &\leq 2^{H_2(d_1/n)n+k-n+1} \varphi \\ &\leq 2^{-1} \varphi. \end{aligned}$$

Let $d = \alpha n$ and $d_1 = \beta n$. The above conditions on k, d and d_1 satisfy if $H_2(\alpha) < \beta$ and $H_2(\alpha) < 1 - H_2(\beta)$. We show that there are α and β that satisfy these inequalities. Choose $\delta_1, \delta_2 < \frac{1}{2}$ such that $H_2(\delta_1) = \frac{1}{2}$ and $H_2(\delta_2) = \delta_1$. Choose $\alpha < \delta_2$. Then $H_2(\alpha) < \delta_1$. Choose β such that $H_2(\alpha) < \beta < \delta_1$. Then $1 - H_2(\beta) > 1 - H_2(\delta_1) = \frac{1}{2} > H_2(\alpha)$. So let $\alpha < H_2^{-1}(H_2^{-1}(1/2)) \approx 0.0146$, where H_2^{-1} is the inverse of the entropy function. With this bound on d, we showed that that there is a weakly self–dual $[n, k, d_1]$ code $\mathcal{C}$ such that $d_1 > k$ and $\mathcal{C}^{\perp}$ is an $[n, k, d]$ code with $k/n \approx H_2(d/n)$. Note that the condition (23) also holds, because the left–hand side of this inequality is at most $2^{n-k+H_2(d/n)n+1}$, which for the chosen value for k, is less than 2^{n-2}. So we have shown the following asymptotic bound.

Theorem 4.9 *For $d < \lambda n$, where $\lambda = H_2^{-1}(H_2^{-1}(1/2))$, there are nonadditive $((n, 2^k, d))$ quantum codes with rate $k/n \geq 1 - 2H_2(d/n)$.*

4.2.2 A strongly nonadditive code

In this section we provide an example of a strongly nonadditive quantum error–correcting code. This is an $((11, 2, 3))$ strongly nonadditive code.

Consider the (Paley type) Hadamard matrix of order 12 (see, e.g., [10], p. 48). Delete the all–1 column and replace -1 by 1 and $+1$ by 0. The result is the following matrix

$$H = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1
\end{bmatrix}.$$

We denote the i^{th} row of H by r_i. The set $\mathcal{C} = \{\, r_i : 1 \leq i \leq 12 \,\}$ is an $(11, 12, 6)$ code. Then a basis for the desired quantum code consists of the following two vectors:

$$\begin{aligned} |0_L\rangle &= \sum_{i=1}^{12} |r_i\rangle \,, \\ |1_L\rangle &= \sum_{i=1}^{12} |\mathbf{1} + r_i\rangle \,, \end{aligned}$$

where $\mathbf{1}$ is the all–1 vector of length 11. We claim these vectors are basis for an $((11, 2, 3))$ quantum code. We have to show that

$$\begin{aligned} \langle 0_L \mid X_\alpha Z_\beta \mid 0_L\rangle &= 0, & (24) \\ \langle 1_L \mid X_\alpha Z_\beta \mid 1_L\rangle &= 0, & (25) \\ \langle 0_L \mid X_\alpha Z_\beta \mid 1_L\rangle &= 0, & (26) \end{aligned}$$

for every $\alpha, \beta \in \{0, 1\}^{11}$ such that $1 \leq \mathrm{wt}(\alpha \cup \beta) \leq 2$. First note that that the distance of any two distinct vectors in the set

$$\{\, r_i : 1 \leq i \leq 12 \,\} \cup \{\, \mathbf{1} + r_i : 1 \leq i \leq 12 \,\}$$

is at least 5. Thus if $1 \leq \mathrm{wt}(\alpha) \leq 4$ then all conditions (24)–(26) hold. Now suppose that $\alpha = \mathbf{0}$. Then (26) trivially holds. To see that (24) and (25) hold it is enough to note that if $1 \leq \mathrm{wt}(\beta) \leq 2$ then $r_i \cdot \beta = 1$ for exactly 6 values of i. This completes the proof that $\{\, |0_L\rangle \,, |1_L\rangle \,\}$ is a basis for an $((11, 2, 3))$ quantum error–correcting code.

To show that this code is nonadditive, let $\varphi = (-1)^\lambda X_\alpha Z_\beta$ be any operator in the stabilizer of this code. Since $\varphi\, |0_L\rangle = |0_L\rangle$ and $\varphi\, |r_1\rangle = |\alpha\rangle$, hence $\lambda = 0$ and α should be one of r_i's. Then we should have $\alpha = r_1 = \mathbf{0}$, because for every r_i, $i \neq 1$, there is some j such that $r_i + r_j$ is not equal to any r_k. Therefore, $\varphi = Z_\beta$. Then

$$Z_\beta\, |0_L\rangle = \sum_{i=1}^{12} (-1)^{r_i \cdot \beta}\, |r_i\rangle = \sum_{i=1}^{12} |r_i\rangle$$

implies that $r_i \cdot \beta = 0$, for every i. But the set $\{\, r_i : 1 \leq i \leq 12 \,\}$ has rank 11, so $\beta = \mathbf{0}$. This shows that the identity operator is the only operator in the stabilizer of this code. Finally, suppose that $X_\alpha T$ is in the generalized stabilizer of this code, where the operator T is of the form (17). Note that the operator T only effects the phases of the states, so the above argument also implies $\alpha = \mathbf{0}$. Now Theorem 4.5 implies that this code is strongly nonadditive.

5 Concluding Remarks

We gave a characterization of additive quantum codes, and showed that there are nonadditive codes with different minimum distances. We showed that nonadditive codes that correct t errors can reach the asymptotic rate $R \geq 1 - 2H_2(2t/n)$. We introduced the notion of strongly nonadditive codes, and gave an example of such codes. It would be interesting to find more examples of such codes. We conjecture that the nonadditive codes constructed in Secition 4.2.1 are also strongly nonadditive codes.

References

[1] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, "Mixed state entanglement and quantum error correction," *Phys. Rev. A*, Vol. 54, No. 5, pp. 3824–3851 (1996).

[2] M. Grassl and Th. Beth, "A note on non–additive quantum codes," LANL e–print quant–ph/97030126.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," LANL e–print quant–ph/9605005.

[4] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," LANL e–print quant–ph/9608006.

[5] A. R. Calderbank and P. W. Shor, "Good quantum error–correcting codes exit," *Phys. Rev. A*, Vol. 54, No. 2, pp. 1098–1105 (1996).

[6] R. Cleve, "Quantum stabilizer codes and classical linear codes," LANL e–print quant–ph/9612048.

[7] D. Gottesman, "A class of quantum error–correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, Vol. 54, No. 3, pp. 1862–8168 (1996).

[8] E. Knill and R. Laflamme, "A theory of quantum error–correcting codes," LANL e–print quant–ph/9604034.

[9] F. J. MacWilliams, N. J. Sloane and J. P. Thompson, "Good self dual codes exist," *Discrete Math.*, vol. 3, pp. 153–162 (1972).

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North–Holland, New York, 1977.

[11] E. M. Rains, "Quantum shadow enumerators," LANL e–print quant–ph/9611001.

[12] E. M. Rains, "Quantum codes of minimum distance two," LANL e–print quant–ph/9704043.

[13] E. M. Rains, R. H. Hardin, P. Shor and N. J. A. Sloane, "A nonadditive quantum code," LANL e–print quant–ph/9703002.

[14] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, Vol. 77, No. 5, pp. 793–797 (1996).

[15] F. Vatan, V. P. Roychowdhury and M. P. Anantram, "Spatially correlated qubit errors and burst–correcting quantum codes," LANL e–print quant–ph/9704019.